UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,158	11/13/2003	Keith Sinclair	50325-0811	2371

29989 7590 06/03/2009

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
STRANGE, AARON N	

ART UNIT	PAPER NUMBER
2448	

MAIL DATE	DELIVERY MODE
06/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/714,158	**Applicant(s)** SINCLAIR ET AL.	
	Examiner AARON STRANGE	**Art Unit** 2448	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-20,22-30 and 32-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *11-14 and 32-35* is/are allowed.

6)☒ Claim(s) *1-9,15-20 and 22-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *20090506*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see page 18, filed 2/25/2009, with respect to the rejection of claims 11 and 32 under 35 U.S.C. § 103(a) have been fully considered and are persuasive. The rejection of claims 11-14 and 32-35 has been withdrawn.

2. Applicant's remaining arguments filed 2/25/2009 have been fully considered but they are not persuasive.

3. With regard to claim 1, and Applicant's assertion that "Feridun does not provide the two kinds of rules recited in claim 1" (Remarks 16), the Examiner respectfully disagrees.

Feridun discloses a "symptom event rule" that "indicates whether events are symptoms of anything" since all incoming events are checked against the registration list to see if any module expressed interest in the event (i.e., whether it is a symptom of something of interest to the registering module) (col. 8, ll. 15-22).

Feridun further discloses a "problem-diagnosis rule" (correlation rule) since groups of events may be correlated to identify a "situation" consisting of several symptomatic events (col. 9, ll. 1-11). Therefore, the correlation rules identify problems occurring when a particular group of symptoms are identified.

With regard to Applicant's assertion that Feridun requires matching all events against all the correlation rules (Remarks 16), the Examiner respectfully disagrees.

Feridun clearly discloses that events failing to match a registration bypass the correlation engine and are not matched with the correlation rules at all (col. 8, ll. 19-24).

4. With further regard to claim 1, and Applicant's assertion that "Feridun teaches away from an approach in which a user can request employing a particular rule in managing a second network" Remarks 17), the Examiner respectfully disagrees. The portion of Feridun relied upon by Applicant in support of this assertion merely states that "some or all" of the modules are loaded depending on configuration data, and that the module configures itself at startup. This has nothing to do with and certainly fails to teach away from permitting a user to employ a particular rule in managing a separate network. The fact that modules may configure themselves at startup does not teach away from a user modifying a configuration or adding a new rule using the remote site management capabilities of Feridun (Col. 4, ll. 10-24).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-9, 11-15, 17-20, 22, 24-30 and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feridun et al. (US 6,336,139) in view of Muthiyan et al. (US 7,328,260) further in view of Zhou et al. (US 7,379,999).

7. With regard to claim 1, Feridun discloses a method for rule-based network management, the method comprising the computer-implemented steps of:

a network management computer defining and storing a set of rules, wherein the set of rules includes:

a symptom-event rule that identifies as a symptom a particular event occurring within a first network in a plurality of networks (events matching the registration list are sent to the correlation engine)(col. 8, ll. 15-22); and

a problem-diagnosis rule that defines a problem within the network as a correlation between one or more symptoms (correlation engine contains correlation rules that identifies situations based on symptomatic events) (col. 9, ll. 1-14);

wherein a symptom comprises an indication of a problem in a network element that results from an event occurring or being true of pertinent data exceeding a threshold (symptoms comprise indications of status changes in the network, which may be indicative of problems in the network)(col. 2, ll. 1-3; col. 3, ll. 21-27);

wherein a problem comprises a certain set of symptoms that occur a prescribed number of times (col. 9, ll. 39-40);

the network management computer collecting and storing symptom-related data about one or more symptoms (events are collected in the input queue)(col. 8, ll. 15-17), wherein collecting and storing the symptom-related data includes monitoring the network for one or more network events identified in the symptom-event rule (events are compared to the registration list and matching events are forwarded to the correlation engine)(col. 8, ll. 15-22); and

the network management computer detecting a problem within the network, wherein detecting the problem includes applying the problem-diagnosis rule to the symptom-related data (correlated events may be used to detect situations, including problems)(col. 9, ll. 5-14 and 41-47);

the network management computer receiving a request from a user to employ a particular rule in managing a second network, separate from the first network (system is used to manage a large distributed environment comprising a plurality of networks, each with its own management server)(col. 4, ll. 10-24); and

distributing, to a device on the second network, the particular rule (managing the second network will necessarily require distributing the rules to nodes on the second network).

Feridun fails to specifically disclose that the rules are stored in one or more Rule-Based Markup Language documents including tags for defining the rule elements or that a problem comprises a set of symptoms occurring in a specified time interval.

Muthiyan discloses a similar system for monitoring a network based on a plurality of rules (Abstract). Muthiyan teaches storing the rules in Rule-Based Markup Language (XML) file including tags for defining the rule elements (col. 48, ll. 23-67). This would have been an advantageous addition to the system disclosed by Feridun since it would have allowed the rules to be edited using a standard text editor (Muthiyan; col. 12, ll. 15-19), eliminating the need for specialized editors to change or view the current rules.

Zhou discloses a similar system for monitoring events on a network (Abstract). Zhou teaches monitoring for a number of occurrences of a particular even in a certain time interval (col. 20, ll. 51-52). This would have been an advantageous addition to the system disclosed by Feridun since it would have allowed the system to monitor for problems associated with events that occur numerous times in a time interval. For example, a general threshold rule that is triggered upon receipt of a million packets would not necessarily be indicative of a problem. However, if a million packets were received at a node in 30 seconds, it may be indicative of a denial of service attack. Allowing Feridun’s threshold rules to be further defined using intervals would enable detection of these problem types.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the Feridun's rules in a Rule-Based Markup Language file to permit the rules to be easily viewed and edited using standard text editors and to allow threshold rules to be further defined using time intervals to enable detection of time-dependent problems such as denial of service attacks.

8. With regard to claim 3, Feridun further teaches and/or suggests storing the rules in a rule repository, wherein the rule repository includes one or more directories containing the rule documents (rules are stored in the registration list containing a

directory of rules indicating interest in a particular event; Rules are also stored in the event correlator)(col. 8, ll. 15-22; col. 9, ll. 1-14).

9. With regard to claim 4, Feridun, when considered in combination with Muthiyan's teaching of XML rule files, further teaches and/or suggests:

a problem-definition tag describing a problem (identification of the "situation") (col. 9, ll. 9-11); and

a correlation tag identifying the correlation between one or more symptoms, wherein the one or more symptoms are defined in one or more symptom tags that include one or more pre-defined indicators associated with the one or more symptoms (correlation rules identify a problem [situation] based on a series of symptomatic events occurring)(col. 9, ll. 41-47).

10. With regard to claim 5, Feridun further teaches and/or suggests that the step of detecting a problem within the network further comprises the steps of:

comparing the symptom-related data to the one or more pre-defined indicators associated with a particular symptom to determine whether the particular symptom exists in the symptom-related data (a first rule is applied to an event stream)(col. 9, ll. 42-45);

repeating the step of comparing the symptom-related data for all symptoms identified in the correlation tag of the RBML document storing the problem-diagnosis rule (a second rule is applied to a second event stream)(col. 9, ll. 45-46); and only if all symptoms identified in the correlation tag exist, determining that the problem identified in the problem-definition tag is detected (if both rules are satisfied, the situation defined by the correlation rule has occurred, and appropriate action is taken)(col. 9, ll. 52-57).

11. With regard to claim 6, Feridun, when considered in combination with Muthiyan's teaching of XML rule files, further teaches and/or suggests:

an event tag identifying the particular event occurring on the network (incoming events are identified and sent to the input queue)(col. 8, ll. 15-22); and

a symptom tag identifying a symptom as a generalized abstraction of the particular event (particular events are sent to the correlation engine if they match an entry in the registration list)(col. 8, ll. 19-22).

12. With regard to claim 7, Feridun, when considered in combination with Muthiyan's teaching of XML rule files, further teaches and/or suggests:

a profile tag identifying a particular network device; and

a command tag identifying a data-collection command, wherein the data collection command, when executed on the particular network device, returns symptom related data associated with the particular network device (distributed monitors may execution data collection commands in response to status requests)(col. 7, ll. 50-56).

13. With regard to claim 8, Feridun further teaches and/or suggests that

the set of rules further includes a problem-correction rule defining one or more corrective actions capable of correcting the problem within the network; and

the method further comprises the step of recommending to a user one or more corrective actions defined in a RBML document storing the problem-correction rule (actions are triggered in response to identification of a problem)(col. 9, ll. 41-57).

14. With regard to claim 9, Feridun further teaches and/or suggests applying to a network device, without user intervention, one or more corrective actions defined in the problem-correction rule (i.e., issuing an event to a network node or starting a new software agent)(col. 9, ll. 54-57).

15. Claims 15, 17-20, 22 and 24-30 are rejected under the same rationale as claims 1 and 3-9, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

16. Claims 2, 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feridun et al. (US 6,336,139) in view of Muthiyan et al. (US 7,328,260) further in view of Zhou et al. (US 7,379,999) further in view of Official Notice.

17. With regard to claim 2, while the system disclosed by Feridun and Muthiyan shows substantial features of the claimed invention (discussed above), it fails to

disclose reviewing the set of rules to identify and resolve a conflict between two or more rules in the set.

The Examiner takes Official Notice that reviewing rule sets to identify and resolve conflicts in old and well known in the art. The advantages of doing so, such as ensuring that the rules behave in the expected manner by eliminating conflicting actions, would have been apparent to one of ordinary skill in the art.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to review the rules to identify and resolve any conflicts between rules.

18. Claims 16 and 23 are rejected under the same rationale as claim 2, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

Allowable Subject Matter

19. Claims 11-14 and 32-35 are allowed.

Conclusion

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AARON STRANGE whose telephone number is (571)272-3959. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Firmin Backer can be reached on 571-272-6703. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aaron Strange/
Examiner, Art Unit 2448